

IPCAMW45 User's Manual



4XEM™
IP Surveillance Solutions



Product name:	Network Camera (IPCAMW45)
Release Date:	2007/06/05
Manual Revision:	1.2
Web site:	http://www.4xem.com/
Email:	mailto:technical@4xem.com mailto:sales@4xem.com
Made in Taiwan.	©Copyright 2007-2012. All rights reserved



IP Surveillance Solutions

Table of Contents

Before You Use This Product	1
Package Contents	2
Installation	3
Hardware Installation	3
Software Installation.....	4
Initial Access to the Network Camera	5
Check Network Settings.....	5
Add Password to Prevent Unauthorized Access.....	5
How To Use	
Installing Plug-in	6
Primary User's Capability.....	7
Main Screen with Camera View	7
Digital Zoom	7
Snapshot	8
Client Settings	8
Digital Output	9
Administrator's Capability	
Fine-tuning for Best Performance	10
Opening Accounts For New Users	12
Build a Security Application	13
Software Revision Upgrade	14
Configuration	15
System Parameters	16
Security Settings	17
Network Settings.....	18
Network Type	18
HTTP	19
RTSP Streaming.....	19
DDNS.....	19
Access List.....	20
Audio and Video	
General	21
Video Settings	21



IP Surveillance Solutions

Video Orientation	22
Audio settings	22
Image Settings	22
Email & FTP	
Email	23
FTP	24
Motion Detection	25
Application Settings	26
Snapshot	26
Video Clip	28
Digital Output	30
System Log	31
Viewing System Parameters	32
Maintenance	32
Appendix	
A. Troubleshooting	33
Status LED	33
Reset and Restore	33
B. URL Commands of the Network Camera	34
Get server parameter values	34
Set server parameter values	35
Available parameters on the server	36
Application page CGI command	45
Capture single snapshot	47
Account management	48
System Logs	49
Configuration file	49
Upgrade Firmware	50
C. Technical Specifications	51
Technology License Notice	52
Electromagnetic Compatibility (EMC)	53
Liability	53


Before You Use This Product

The use of surveillance devices may be prohibited by law in your country. The Network Camera is not only a high-performance web-ready camera but also can be part of a flexible surveillance system. It is the user's responsibility to ensure that the operation of such devices is legal before installing this unit for its intended use.

It is important to first verify that all contents received are complete according to the list in the "Package Contents" chapter. Take notice of the warnings in the "Quick Installation Guide" before the Network Camera is installed, then carefully read and follow the instructions in the "Installation" chapter to avoid damages due to faulty assembly and installation. This also ensures the product is used as intended.

The Network Camera is a network device and its use should be straightforward for those who have basic network knowledge. The "Troubleshooting" chapter in the Appendix provides remedies to the most common errors in set up and configuration. You should consult this chapter first if you run into a system error.

The Network Camera is designed for various applications including video sharing, general security/surveillance, etc. The "How to Use" chapter suggests ways to best utilize the Network Camera and ensure proper operations. For the creative and professional developers, the "URL Commands of The Network Camera " chapter serves to be a helpful reference to customize existing homepages or integrating with a current web server.

For paragraphs preceded by  the reader should use caution to understand completely the warnings. Ignoring the warnings may result in serious hazards or injuries.

Package Contents

IPCAMW45



Software CD



Quick installation guide



Power adapter



Camera stand



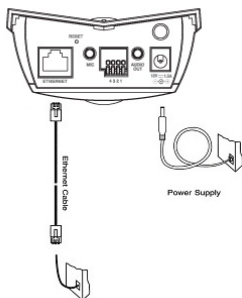
Warranty card



Installation

In this manual, "User" refers to whoever has access to the Network Camera, and "Administrator" refers to the person who can configure the Network Camera and grant user access to the camera.

Hardware Installation





Using the Power Adapter as power source:

1. Plug the Ethernet cable into the Network Camera.
2. Connect the Power Adapter to the Network Camera.
3. Plug the Power Adapter into electrical outlet.
4. Observe LED status lights (status light progression specified below).

Using Power over Ethernet PoE as power source:

1. Connect one end of Ethernet cable to 12V PoE injector (purchased separately).
2. Connect the other end of Ethernet cable to the Network Camera.
3. Observe LED status lights (status light progression specified below).

 The Ethernet cable should meet the specs of UTP category 5 and not exceed 100 meters in length.

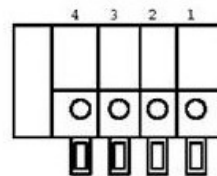
 The Power Adapter is not used when powering with PoE.

Status LED Color	Description
Blinking Red	Power is being supplied to the camera.
Steady Green	The camera is booting up.
Blinking Orange & Green	The camera is trying to obtain an IP address.
Steady Orange	An IP address is successfully assigned to the camera.
Blinking Orange & Red	The camera is working.
Fast Blinking Orange & Red	During firmware upgrading.

Proceed to software installation when the LED status light blinks orange & red.

Digital Input/Output Terminal

This Network Camera provides a general I/O terminal block with one digital input and one digital output device control.



1. Digital output
2. Digital input
3. DC power
4. Ground

Software Installation

When the hardware installation is complete, users can use the Installation Wizard program included in the product CDROM to find the location of the Network Camera. There may be many Network Cameras in the local network. Users can differentiate the Network Cameras with the serial number. The serial number is printed on the labels on the carton and the back of the Network Camera body. Please refer to the user's manual for the Installation Wizard for more details.

Once the installation is complete, the Administrator should proceed to the next section "Initial access to the Network Camera" for necessary checks and configurations.

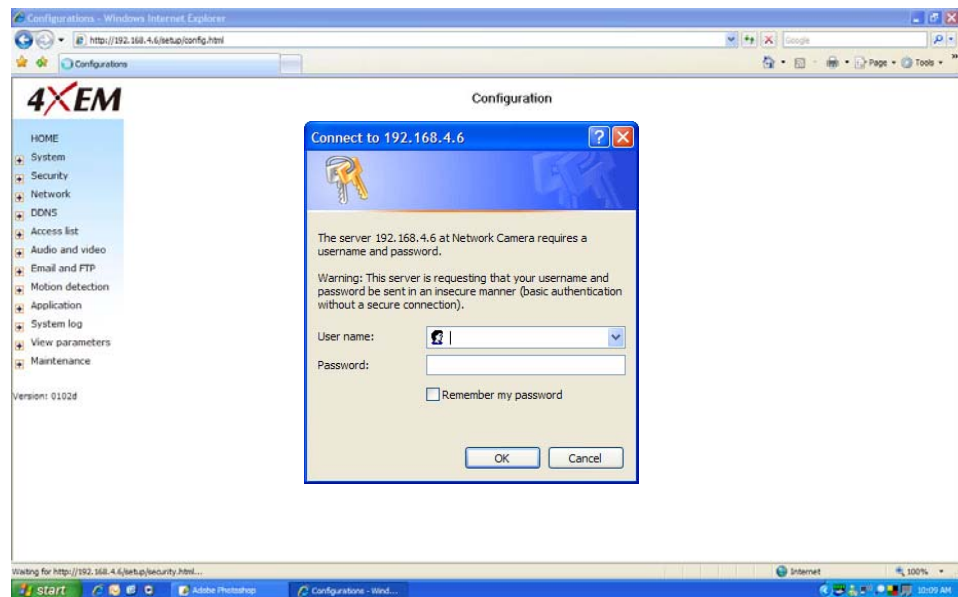
Initial Access to the Network Camera

Check Network Settings

The Network Camera can be connected either before or immediately after software installation onto the Local Area Network. The Administrator should complete the network settings on the configuration page, including the correct subnet mask and IP address of the gateway and the DNS Servers. Ask your network administrator or Internet service provider for the details. If any setting is entered incorrectly and you cannot proceed with setting up the Network Camera, restore the factory settings following the steps in the "Troubleshooting" chapter in the Appendix.

Add Password to Prevent Unauthorized Access

The default Administrator's password is blank and the Network Camera initially will not ask for any password. The Administrator should immediately assign a new password as a matter of prudent security practice. Once the Administrator's password is saved,



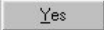
the Network Camera will ask for the user's name and password before each access. The Administrator can set up a maximum of twenty (20) user accounts. Each user can access the Network Camera except to perform system configuration. Some critical functions such as system configuration, user administration, and software upgrades are accessible only by the Administrator. The user name for the Administrator is permanently assigned as "root". Once the password is changed, the browser will display an authentication window to ask for the new password. **Once the password is set, there is no provision to recover the Administrator's password. The only option is to restore to the original factory default settings.**

How to Use

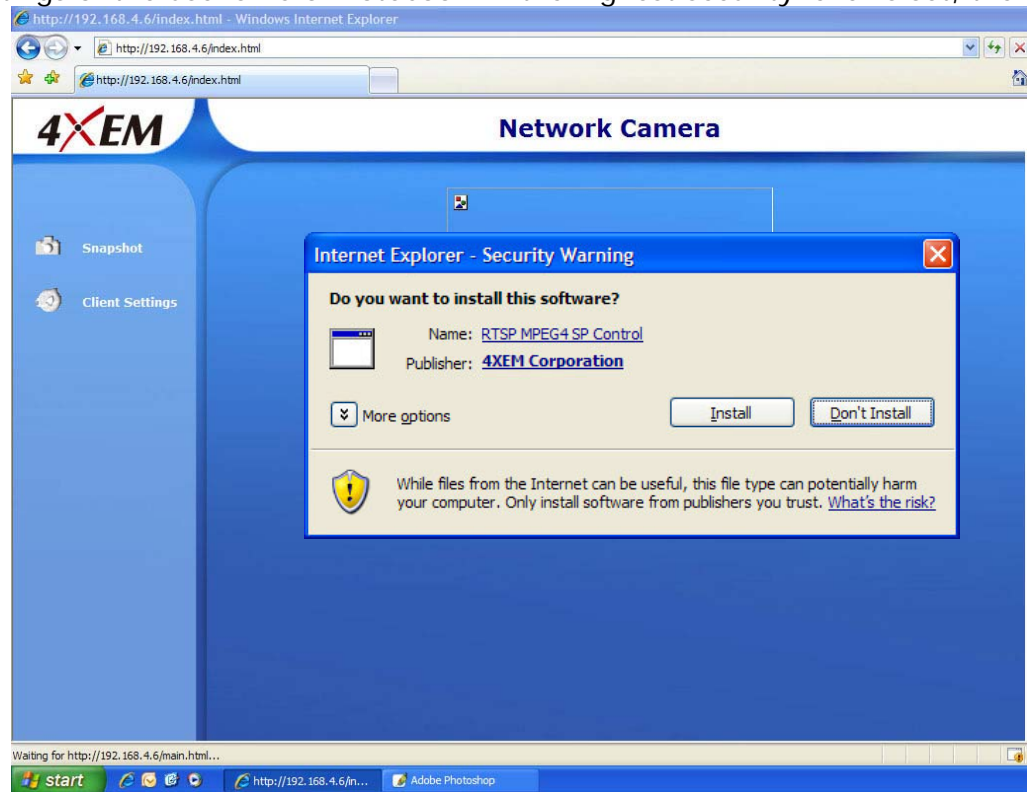
Installing Plug-in

For the initial access to the Network Camera in Windows, the web browser may prompt for permission to install a new plug-in for the Network Camera. Permission request depends on the Internet security settings of the user's PC or notebook. If the highest security level is set, the computer may prohibit any installation and execution attempt.

This plug-in has been registered for certificate and is used to display the video in the browser. Users may click on

 to proceed. If the web browser does not allow the user to continue to install, check the

Internet security option and lower the security levels or contact your IT or networking supervisor for help.



Primary User's Capability

Main Screen with Camera View

Snapshot: Opens a still picture of current view in new window.

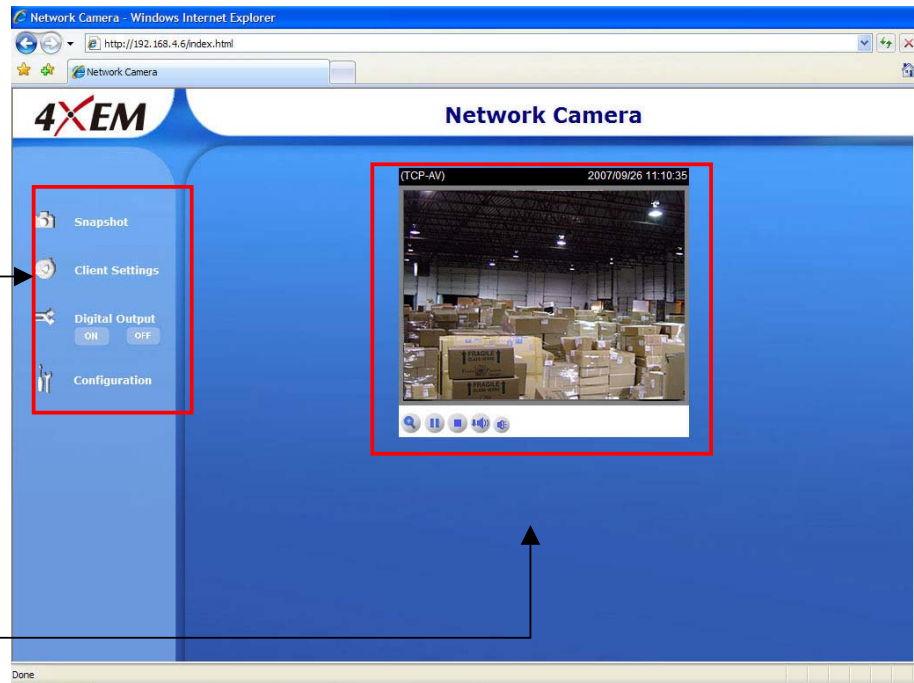
Client Settings:

Configures local Browser settings.

Configuration:

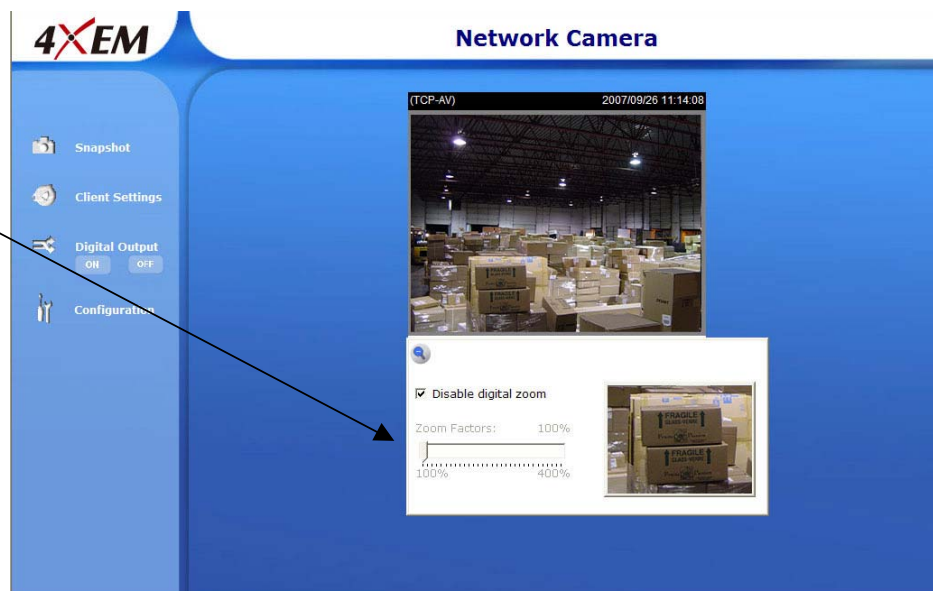
Provides access to all camera configuration options.

Camera View: Live streaming video.



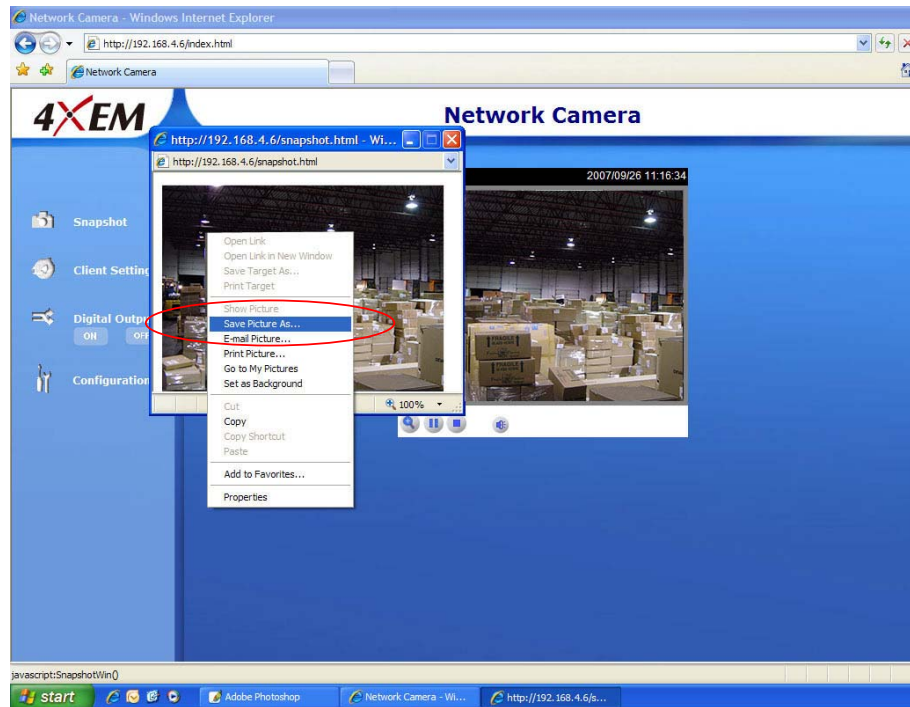
Digital Zoom

Click on the magnifier icon under the camera view then the digital zoom control panel will be shown. Uncheck "Disable digital zoom" and use the slider control to change the zoom factors.



Snapshot

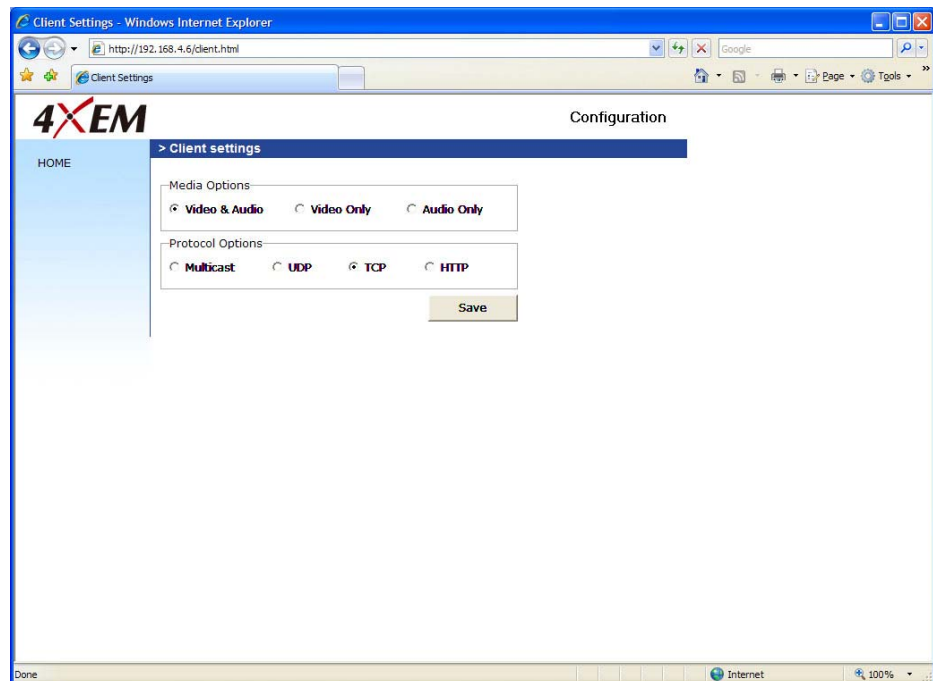
Click on **Snapshot**, web browser will pop up a new window to show the snapshot. Users can point at the snapshot and click the right mouse button to save it.



Client Settings

There are two settings for the client side:

Media Options to determine the type of media to be streamed and **Protocol Options** which allows choice of connection protocol between client and server. There are two protocol choices to optimize your usage – UDP and TCP.





IP Surveillance Solutions

The **UDP** protocol allows for more real-time audio and video streams. However, some packets may be lost due to network burst traffic and images may be obscured. The **TCP** protocol allows for less packet loss and produces a more accurate video display. The downside with this protocol is that the real-time effect is worse than that with the UDP protocol. If no special need is required, UDP protocol is recommended. Generally speaking, the client's choice will be in the order of UDP – TCP.

After the Network Camera is connected successfully, **Protocol Option** will indicate the selected protocol. The selected protocol will be recorded in the user's PC and will be used for the next connection. If the network environment is changed, or the user wants to let the web browser detect again, manually select the UDP protocol, save, and return HOME to re-connect.

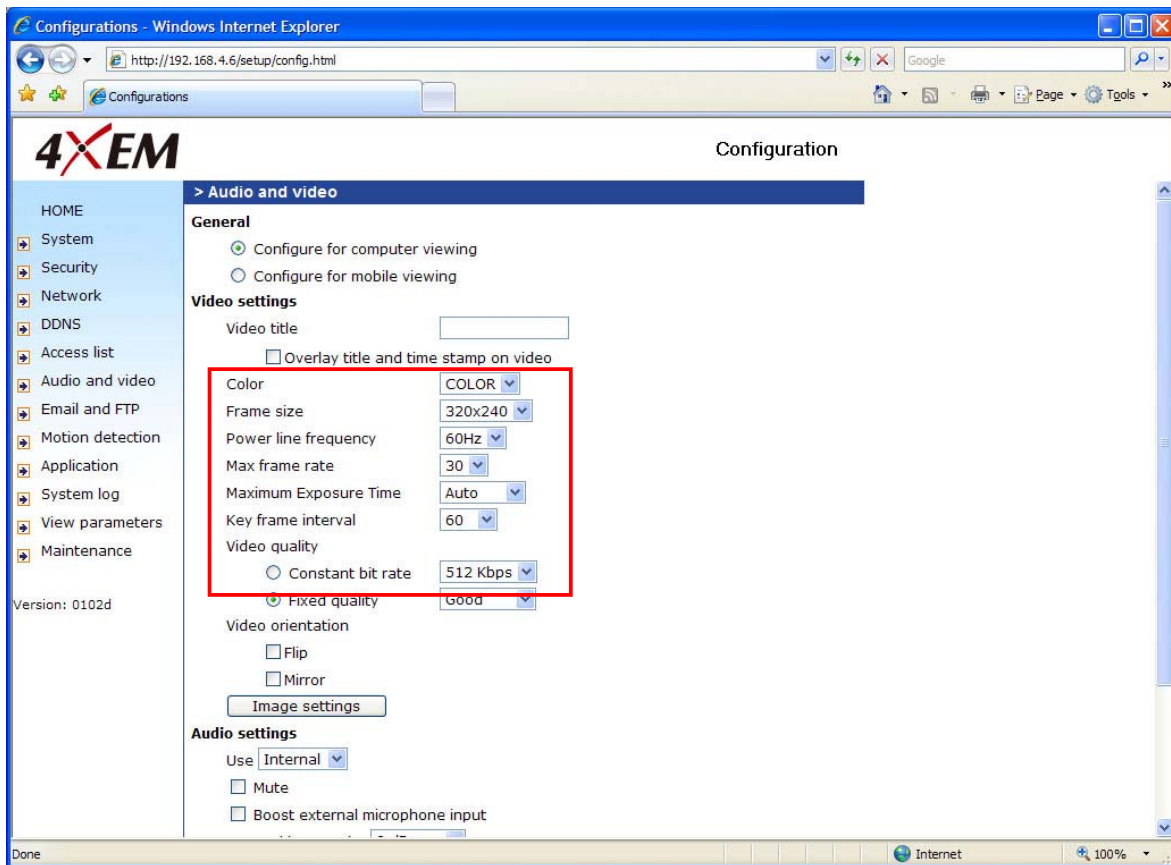
Digital Output

Click on **ON**, the digital output of the Network Camera will be triggered. Or, clicking on **OFF** can let the digital output turn into normal state.

Administrator's Capability

Fine-tuning for Best Performance

Best performance generally equates to the fastest image refresh rate with the best video quality, and at the lowest network bandwidth as possible. The three factors, **Maximum frame rate**, **Constant bit rate**, and **Fix quality** on the Audio and Video Configuration page, correlate to allow for achieving the best performance possible.



For Viewing by Mobile Phone

Most 3GPP cell phone supports media streaming with MPEG4 video and GSM-AMR audio. Due to the limitation of the bandwidth for 3GPP, only 176x144 video solution will be supported for cell phone viewing. Select the **Configure for mobile viewing** option will change the range of other related video settings.

For Best Real-time Video Images

To achieve good real-time visual effect, the network bandwidth should be large enough to allow a transmission rate of greater than 20 image frames per second. If the broadband network is over 1 Mbps, set the **Fix bit rate** to 1000Kbps or 1200Kbps, and set **Fix quality** at the highest quality. The maximum frame rate is 30. If your network bandwidth is more than 512Kbps, you can fix the bit rate according to your bandwidth and set the maximum frame rate to 30 fps. If the images vary dramatically in your environment, you may want to slow the maximum frame rate down to 20 fps in order to lower the rate of data transmission. This allows for better video quality and the human eyes cannot readily detect the differences between 20, 25, or 30 frames per second. If your network bandwidth is below 512 Kbps, set the **Fix bit rate** according to your bandwidth and try to get the best performance by fine-tuning with the **Maximum frame rate**. In a slow network, greater frame rate results in blur images. Another work-around is to choose **160x120** in the **Size** option for better images. Video quality performance will vary somewhat due to the number of users viewing on the network, even when the parameters have initially been finely tuned. Performance will also suffer due to poor connectivity because of the network's burst constraint.

Only Quality Images Will Do

To have the best video quality, you should set **Fix quality** at **Detailed** or **Excellent** and adjust the **Maximum frame rate** to match your network's bandwidth. If your network is slow and you receive "broken" pictures, go to the TCP protocol in **Connection type** and choose a more appropriate mode of transmission. The images may suffer a time delay due to a slower connection. The delay will also increase with added number of users.

Somewhere Between Real-time and Clear Images

If you have a broadband network, set **Fix quality** at **Normal** or better, rather than setting **Fix bit rate**. You can also fix the bandwidth according to your actual network speed and adjust the frame rate. Start from 30 fps down for best results but not below 15 fps. If the image qualities are not improved, select a lower bandwidth setting.

Opening Accounts For New Users

The screenshot shows the 4XEM Configuration web interface in a Windows Internet Explorer browser window. The address bar shows the URL <http://192.168.4.6/setup/config.html>. The page title is "Configurations - Windows Internet Explorer". The main content area is titled "Configuration" and has a sidebar menu on the left with options: HOME, System, Security, Network, DDNS, Access list, Audio and video, Email and FTP, Motion detection, Application, System log, View parameters, and Maintenance. The "Security" section is expanded, showing three sub-sections highlighted with red boxes and numbered 1, 2, and 3:

- Root password** (Box 1): Includes a note "* Blank root password will disable user authentication", a "Root password" input field, a "Confirm password" input field, and a "Save" button.
- Add user** (Box 2): Includes a "User name" input field, a "User password" input field, an "Add" button, and a checkbox for "I/O access".
- Manage user** (Box 3): Includes a "User name" dropdown menu (currently showing "-- no user --") and a "delete" button.

At the bottom left of the page, it says "Version: 0102d". The browser status bar at the bottom shows "Done" and "Internet" with a 100% zoom level.

Protect Network Camera by passwords

The Network Camera is shipped without any password by default. That means everyone can access the Network Camera including the configuration as long as the IP address is known. It is necessary to assign a password if the Network Camera is intended to be accessed by others. Type a new word twice in **1** to enable protection. This password is used to identify the administrator. Then add an account with user name and password for your friends in **2**. The Network Camera can provide twenty accounts for your valuable customers or friends. You may delete some users from **3**.

Build a Security Application

The Administrator can use the built-in motion detection to monitor any movement and perform many useful security applications. To upload the snapshots, users can choose either email or FTP according to user's needs. Both e-mail and FTP use the network settings on the Email and FTP page.

1. Click on **Configuration** on homepage,
2. Click on **Motion detection** at the left column,
3. Check **Enable motion detection**,
4. Click on new to have a new window to monitor video,
5. Type in a name to identify the new window,
6. Use the mouse to click, hold, and drag the window corner to resize or the title bar to move,
7. Fine-tune using the **Sensitivity** and **Percentage** fields to best suit the camera's environment. Higher **Sensitivity** detects the slighter motion. Higher **Percentage** discriminates smaller objects,
8. Clicking on **Save** enables the activity display. Green means the motion in the window is under the watermark set by Administrator and red means it is over the watermark,
9. Click on **Application** at the left column,
10. Check the weekdays as you need and give the time interval to monitor the motion detection every day,
11. Select the **Trigger on Motion detection**.
12. Set the **delay before detecting next motion** to avoid continuous false alarms following the original event,
13. Set the number of pre-event and post-event images to be uploaded,
14. Check the window name set in step 5,
15. Check the way to upload snapshot.
16. Click on **save** to validate.

Software Revision Upgrade

Customers can obtain the up-to-date software from the web site of 4XEM. An easy-to-use Upgrade Wizard is provided to upgrade the Network Camera with just a few clicks. The upgrade function is opened to the Administrator only. To upgrade the system, follow the procedures below.

1. Download the firmware file from www.4xem.com.
2. Run the Upgrade Wizard and proceed following the prompts. Refer to the instructions of the Upgrade Wizard for details.
3. Or upgrade firmware from HTTP web page directly
3. The whole process will finish in a few minutes and it will automatically restart the system.



If power fails during the writing process of Flash memory, the program in the memory of the Network Camera may be destroyed permanently. If the Network Camera cannot restart properly, call 4XEM Technical Support.

Configuration

Only the Administrator can access system configuration. Each category in the left column will be explained in the following pages. The bold texts are the specific phrases on the Option pages. The Administrator may type the URL below the figure to directly enter the frame page of configuration. If the Administrator also wants to set certain options through the URL, read the reference appendix for details.

The screenshot shows the 'Configurations - Windows Internet Explorer' window. The address bar displays 'http://192.168.4.6/setup/config.html'. The page title is 'Configurations'. The 4XEM logo is in the top left, and the word 'Configuration' is in the top right. A left sidebar contains a menu with items: HOME, System, Security, Network, DDNS, Access list, Audio and video, Email and FTP, Motion detection, Application, System log, View parameters, and Maintenance. Below the menu, it says 'Version: 0102d'. The main content area is titled '> System'. It contains the following settings: 'Host name' is 'Network Camera'; 'Turn off the LED indicator' is an unchecked checkbox; 'Daylight Saving Time' is an unchecked checkbox; 'Time zone' is a dropdown menu showing 'GMT+08:00 Beijing, Chongqing, Hong Kong, Kuala Lumpur, Singapore, Taipei'; 'Keep current date and time' is a selected radio button; 'Sync with computer time' is an unselected radio button with fields for 'PC date' (2007/11/19) and 'PC time' (10:48:25); 'Manual' is an unselected radio button with fields for 'Date' (2007/09/26) and 'Time' (11:46:37); 'Automatic' is an unselected radio button with fields for 'NTP server' (skip to invoke default server) and 'Update interval' (One hour); 'DI and DO' section includes 'Digital input: normal status is Low', 'Digital output: normal status is Grounded', and an unchecked checkbox for 'Reset digital output after 1 seconds'. A 'Save' button is at the bottom. The status bar at the bottom shows 'Done' and 'Internet'.

System Parameters

Host name: The text displays the title at the top of the main page.

Turn off the LED indicator: Check this option to shut off the LED on the rear. It can prevent the camera's operation being noticed.

Time zone: Adjust the time with that of the time-servers for local settings.

Keep current date and time: Click on this to reserve the current date and time of the Network Camera. An internal real-time clock maintains the date and time even when the power of the system is turned off.

Sync with computer time: Synchronizes the date and time of the Network Camera with the local computer. The read-only date and time of the PC is displayed as updated.

Manual: Adjust the date and time according to what is entered by the Administrator. Notice the format in the related fields while doing the entry.

Automatic: Synchronize with the NTP server over the Internet whenever the Network Camera starts up. It will fail if the assigned time-server cannot be reached.

NTP server: Assign the IP address or domain name of the time-server. Leaving the text box blank connects the Network Camera to the default time-servers.

Update interval: Select hourly, daily, weekly, or monthly update with the time on the NTP server.

Digital input: Select High or Low to define normal status of the digital input.

Digital output: Select Grounded or Open to define normal status of the digital output.

Reset digital output: The check box enable the function of resetting digital output. When the digital output is triggered, after the number time the digital output will reset into normal state.

Remember to click on to immediately validate the changes. Otherwise, the correct time will not be synchronized.

Security Settings

Root password: Change the Administrator's password by typing in the new password identically in both text boxes. The typed entries will be displayed as asterisks for security purposes. After pressing **Save**, the web browser will ask the Administrator for the new password for access.

Add user: Type the new user's name and password and press **Add** to insert the new entry. The new user will be displayed in the user name list. There is a maximum of twenty user accounts. Checking I/O access can enable user to use D/I and D/O applications

Manager user: Pull down the user list to find the user's name and press **Delete** to complete.

The screenshot shows a web browser window titled "Configurations - Windows Internet Explorer" with the address bar displaying "http://192.168.4.6/setup/config.html". The page features the 4XEM logo and a "Configuration" header. A left sidebar lists navigation options: HOME, System, Security, Network, DDNS, Access list, Audio and video, Email and FTP, Motion detection, Application, System log, View parameters, and Maintenance. The main content area is titled "> Security" and contains three sections: "Root password" with fields for "Root password" and "Confirm password" and a "Save" button; "Add user" with fields for "User name" and "User password", an "Add" button, and an unchecked "I/O access" checkbox; and "Manage user" with a dropdown menu showing "-- no user --" and a "delete" button. The version "0102d" is noted at the bottom left of the sidebar.

Network Settings

Any changes made on this page will restart the system in order to validate the changes. Make sure every field is entered correctly before clicking on **Save**.

Network Type

LAN & PPPoE:

The default type is LAN. Select PPPoE if using ADSL

Get IP

address

automatically & Use fixed IP address:

The default
status is **Get IP
address
automatically.**

This can be
tedious having
to perform
software
installation
whenever the
Network
Camera starts.

Therefore, once the network settings, especially the IP address, have been entered correctly, select **Use fixed IP address** then the Network Camera will skip installation at the next boot. The Network Camera can automatically restart and operate normally after a power outage. Users can run IP installer to check the IP address assigned to the Network Camera if the IP address is forgotten or using the UPnP function provided by the Network Camera (MS Windows XP provides UPnP function at **My Network Place**).

IP address: This is necessary for network identification.

Subnet mask: This is used to determine if the destination is in the same subnet. The default value is "255.255.255.0".

Default router: This is the gateway used to forward frames to destinations in a different subnet.



IP Surveillance Solutions

Primary DNS: The primary domain name server that translates hostnames into IP addresses.

Secondary DNS: Secondary domain name server that backups the Primary DNS.

Enable UPnP presentation: Enable the UPnP camera short cut

Enable UPnP port forwarding: Enable uPnP port forwarding

PPPoE: If using the PPPoE interface , fill the following settings from ISP

User name: The login name of PPPoE account

Password: The password of PPPoE account

Confirm password: Input password again for confirmation

HTTP

Http port: This can be other than the default Port 80. Once the port is changed, the users must be notified of the change for the connection to be successful. For instance, when the Administrator changes the HTTP port of the Network Camera whose IP address is 192.168.0.100 from 80 to 8080, the users must type in the web browser "http://192.168.0.100:8080" instead of "http://192.168.0.100".

RTSP Streaming

Access name: This is the access URL for making connection from client software. Using rtsp://<ip address>/<access name> to make connection

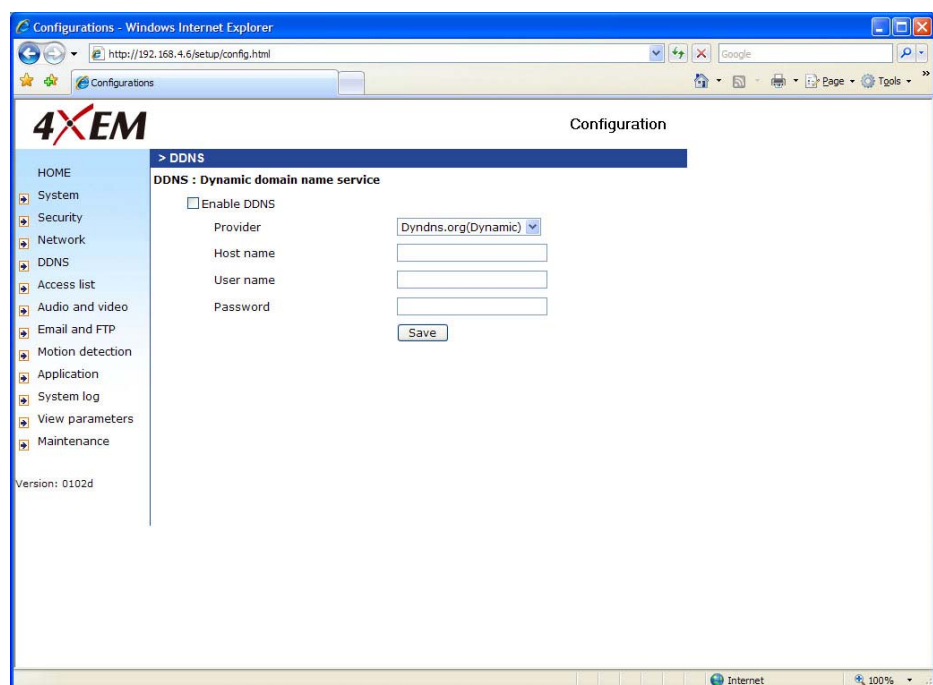
RTSP port: This can be other than the default Port 554

DDNS

Enable DDNS: This option turns on the DDNS function.

Provider: The provider list contains four hosts that provide DDNS services. Please connect to the service provider's website to make sure the service charges.

Host Name: If the User



wants to use DDNS service, this field must be filled. Please input the hostname that is registered in the DDNS server.

Username/E-mail: The Username or E-mail field is necessary for logging in the DDNS server or notify the User of the new IP address. Note: when this field is input as "Username" the following field must be input as "Password".

Password/Key: Please input the password or key to get the DDNS service.

Save: Click on this button to save current settings for the DDNS service and UPnP function.

Access List

The access list is to control the access permission of clients by checking the client IP address.

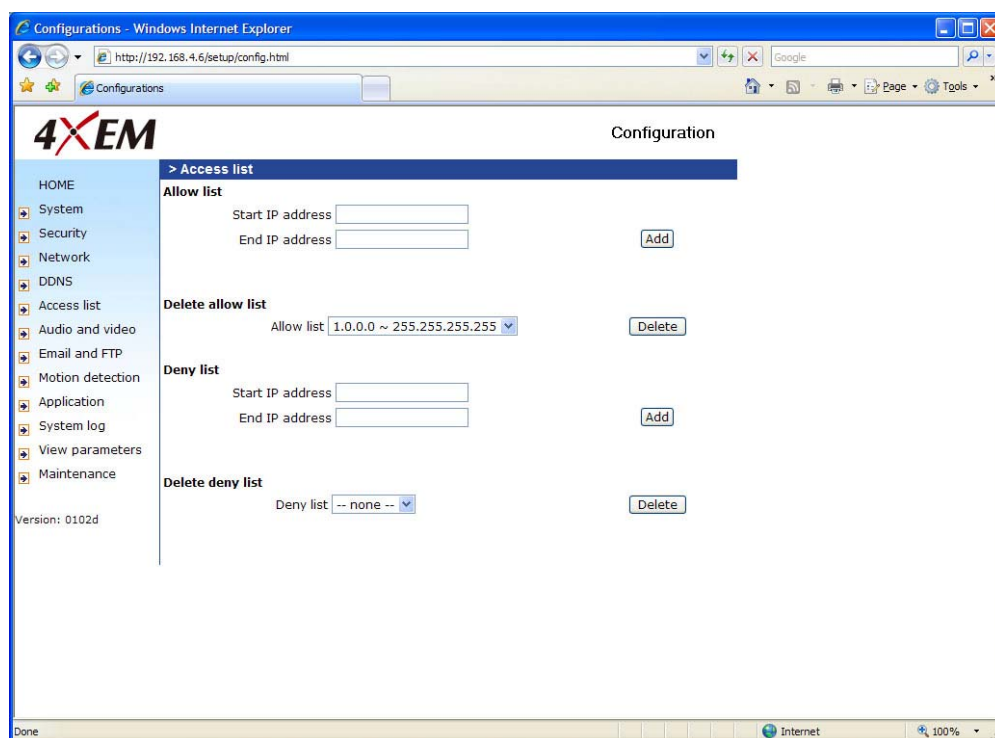
There are two lists for permission control: **Allow List** and **Deny List**.

Only those clients whose IP address is in the **Allow List** and not in the **Deny List** can connect to the Video Server or

Network Camera for receiving the audio/video streaming.

Both **Allow List** and **Deny List** consist of a list of IP ranges. If you want to add a new IP address range, type the **Start IP Address** and **End IP Address** in the text boxes and click on the **Add** button. If you want to remove an existing IP address range, just select from the pull-down menu and click on the **Delete** button.

Both the Allow List and Deny List can have 20 entries.



Audio and Video

General

Configure for computer viewing: To make quick setting for computer viewing.

Configure for mobile viewing: To make quick setting for cell phone viewing.

Video Settings

Video title: The text string can be displayed on video

Color: Select either for color or monochrome video display.

Frame Size: There are four options for video sizes. **160x120, 176x144, 320x240, & 640x480.**

Power line frequency (for fluorescent light):

Change the frequency setting to eliminate uncomfortable flash image when the light source is only fluorescent light.

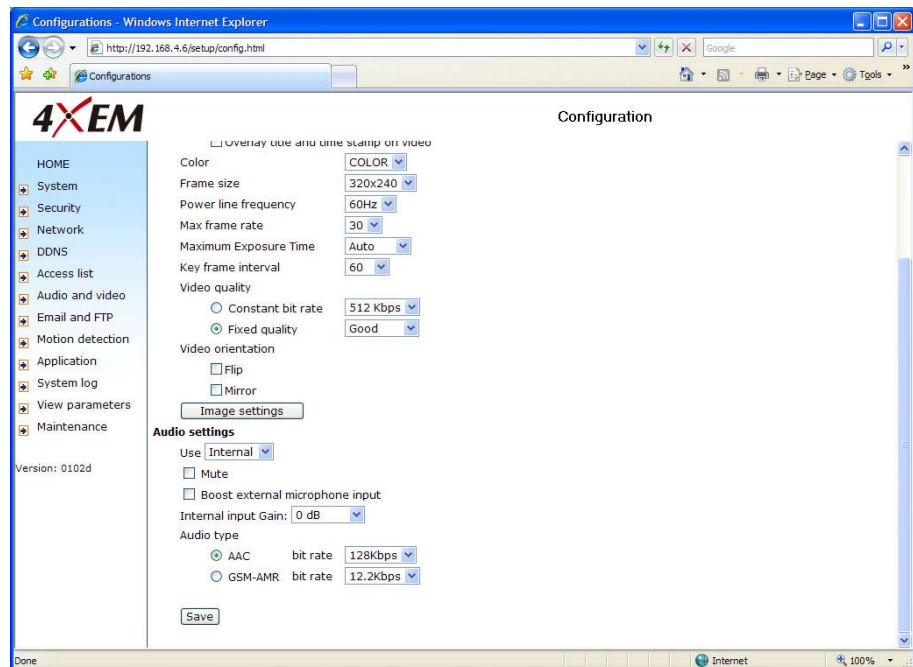
There are three dependent parameters provided for video performance adjustment.

Max frame rate: Allows you to specify the maximum number of frames per second generated by the camera.

Maximum Exposure Time: Adjusts the shutter speed of the camera to allow for exposure adjustments.

Key frame interval: Determines how often full data frames are sent from the camera in the MPEG4 video stream. Lower key frame intervals improve the overall quality of the image at a cost of bandwidth usage and storage requirements.

Video Quality: This section allows you to force the camera to either operate within a certain bandwidth or maintain a certain quality level.



Video Orientation

Flip: Vertically rotate the video.

Mirror: Horizontally rotate the video. Check both options if the Network Camera is installed upside down.

White balance: Adjust the value for best color temperature.

Audio settings

Use: Switch **internal** or **microphone** to set up the source of audio input


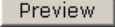

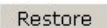
Mute: Audio mute

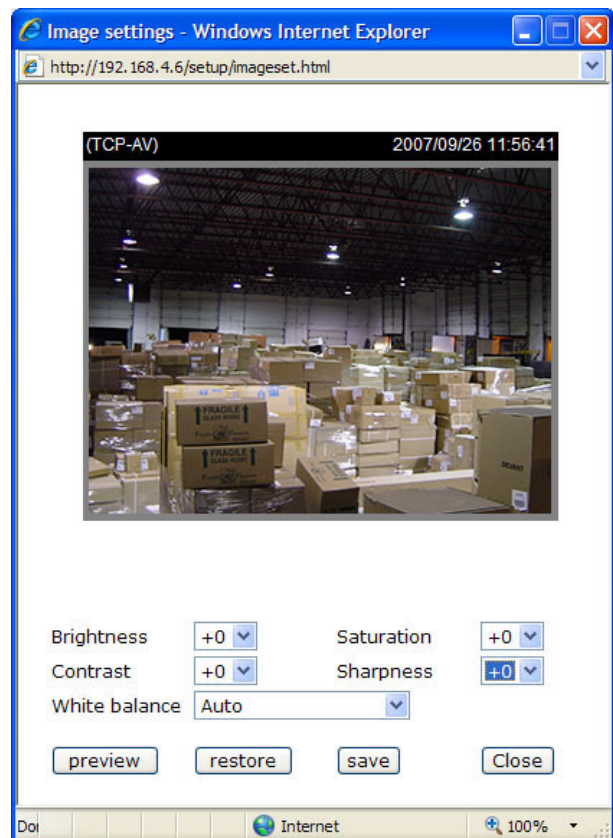
Boost external microphone input: Enhance the gain of the external microphone

Internal input Gain: Modify the gain of the internal audio input

Audio type: Select audio codec **AAC** or **GSM-AMR** and the bit rate

Image Settings

 Click on this button to pop up another window to tune **Brightness**, **Contrast**, **Hue** and **Saturation** for video compensation. Each field has eleven levels ranged from -5 to +5. In **Brightness** and **Contrast** fields the value 0 indicates auto tuning. The user may press  to fine-tune the image. When the image is O.K., press  to set the image settings.  Click on this to recall the original settings without incorporating the changes.



Email & FTP

Email

When the SMTP server supports SMTP authentication, users need to give the valid user name and password to send email via the server.

Sender email address: the email address of the sender.

There are two external mail servers that can be configured: primary and secondary. The network camera will use the primary server as a default, and use the secondary server when the primary server is unreachable.

The screenshot shows the 4XEM Configuration web interface in a Windows Internet Explorer browser. The address bar shows 'http://192.168.4.6/setup/config.html'. The interface has a left sidebar with a tree view containing: HOME, System, Security, Network, DDNS, Access list, Audio and video, Email and FTP (selected), Motion detection, Application, System log, View parameters, and Maintenance. The main content area is titled 'Configuration' and is divided into two sections: 'Email' and 'FTP'. The 'Email' section includes a 'Sender email address' field, a 'Primary email server' section with fields for 'Server address', 'User name', 'Password', and 'Recipient email address', and a 'Secondary email server' section with the same four fields. The 'FTP' section includes a 'Built-in FTP server port number' field with the value '21', a 'Primary FTP server' section with fields for 'Server address', 'FTP server port' (value '21'), 'User name', 'Password', and 'Remote folder name', and a 'Secondary FTP server' section with fields for 'Server address' and 'FTP server port' (value '21'). The status bar at the bottom shows 'Done' and 'Internet'.

Server address: The domain name or IP address of the external email server.

User name: This granted user name on the external email server.

Password: This granted password on the external email server.

Recipient email address: The email address of the recipients for snapshots or log file. Multiple recipients must be separated by a semicolon (;).

FTP

Built-in FTP server port number: This can be other than the default port 21. The user can change this value from 1025 to 65535. After a change, the external FTP client program must change the server port of connection accordingly.

There are two external FTP servers that can be configured: primary and secondary. The network camera will use the primary server as a default, and use the secondary server when the primary server is unreachable.

The screenshot shows the 'Configurations' web page in a Windows Internet Explorer browser. The address bar shows 'http://192.168.4.6/setup/config.html'. The page has a sidebar menu on the left with options: HOME, System, Security, Network, DDNS, Access list, Audio and video, Email and FTP, Motion detection, Application, System log, View parameters, and Maintenance. The main content area is titled 'Configuration' and contains several sections: 'Email' (with fields for Password, Recipient email address, and Secondary email server details), 'FTP' (with a 'Built-in FTP server port number' set to 21), 'Primary FTP server' (with fields for Server address, FTP server port set to 21, User name, Password, and Remote folder name), and 'Secondary FTP server' (with fields for Server address, FTP server port set to 21, User name, Password, and Remote folder name). A 'Save' button is at the bottom right of the FTP section. The version '0102d' is noted in the bottom left of the main area.

Server address: The domain name or the IP address of the external FTP server. The following user settings must be correctly configured for remote access.

FTP server port: This can be other than the default port 21. The user can change this value from 1025 to 65535.

User name: Granted user name on the external FTP server.

Password: Granted password on the external FTP server.

Remote folder name: Granted folder on the external FTP server. The string must conform to that of the external FTP server. Some FTP servers cannot accept preceding slash symbol before the path without virtual path mapping. Refer to the instructions for the external FTP server for details. The folder privilege must be open for upload.

Motion Detection

Enable motion detection: Check this option to turn on motion detection.

New Click on this button to add a new window. At most three windows can exist simultaneously. Use the mouse to click, hold, and drag the window frame to resize or the title bar to move. Clicking on the 'x' at the upper right-hand corner of the window to delete the window. Remember to save in order to validate the changes.

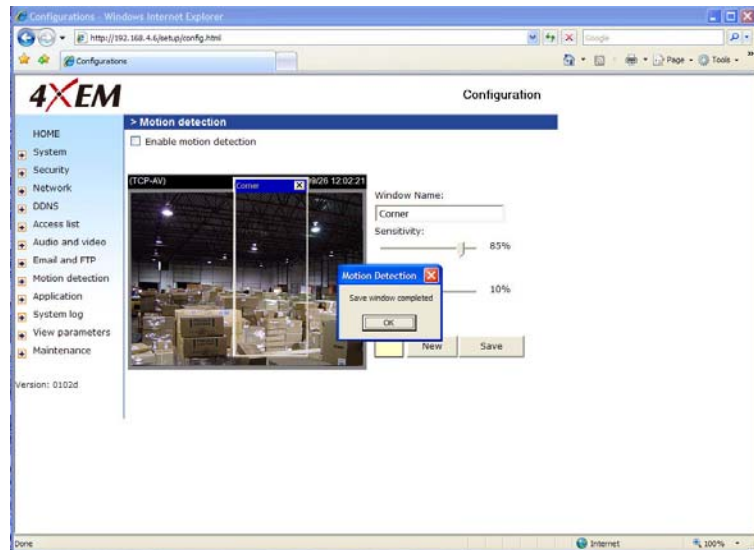
Save Click on this button to save the related window settings. A graphic bar will rise or fall depending on the image variation. A green bar means the image variation is under monitoring level and a red bar means the image variation is over monitoring level. When the bar goes red, the detected window will also be outlined in red. Going back to the homepage, the monitored window is hidden but the red frame shows when motion is detected.

Window Name: The text will show at the top of the window.

Sensitivity: This sets the endurable difference between two sequential images.

Percentage: This sets the space ratio of moving objects in the monitoring window. Higher sensitivity and small percentage will allow easier motion detection.

The following figure shows the screen when **Save** is clicked. The monitoring window has been outlined in red and the graphic bar goes red since the goldfish is moving.



Application Settings

Application

There are four Applications available: two snapshots, one video clip and one digital input, all with the following settings.

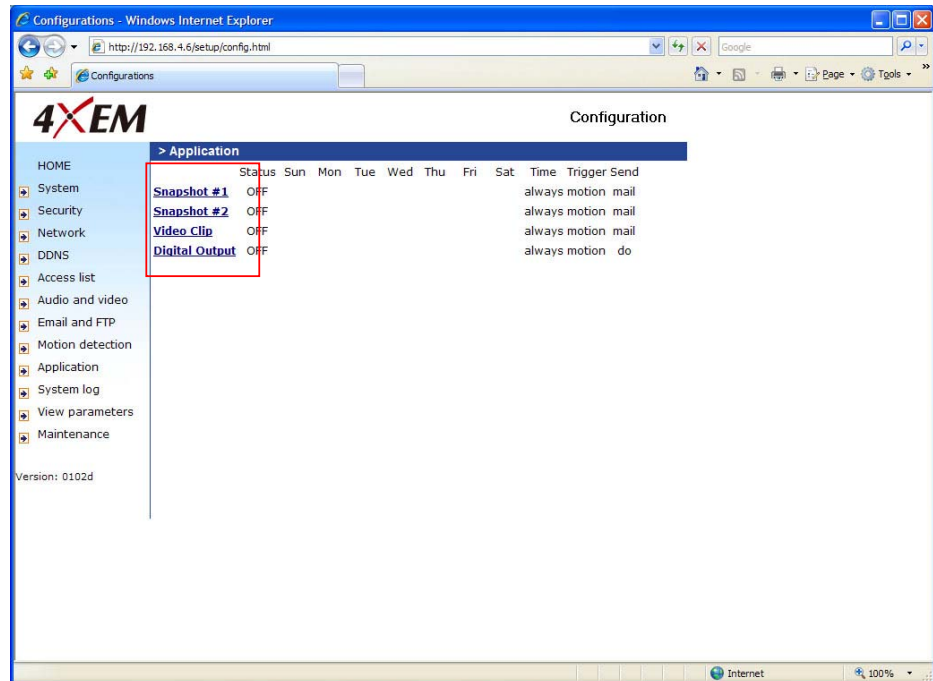
Status: ON/OFF show the status of application.

Sun - Sat: Select the days of the week to perform the application.

Time: Show **Always** or input the time interval.

Trigger: Event trigger type has digital input, motion detection and is sequential.

Send: After Event has been triggered, IP cam will send something by email, ftp or trigger digital output.



Snapshot

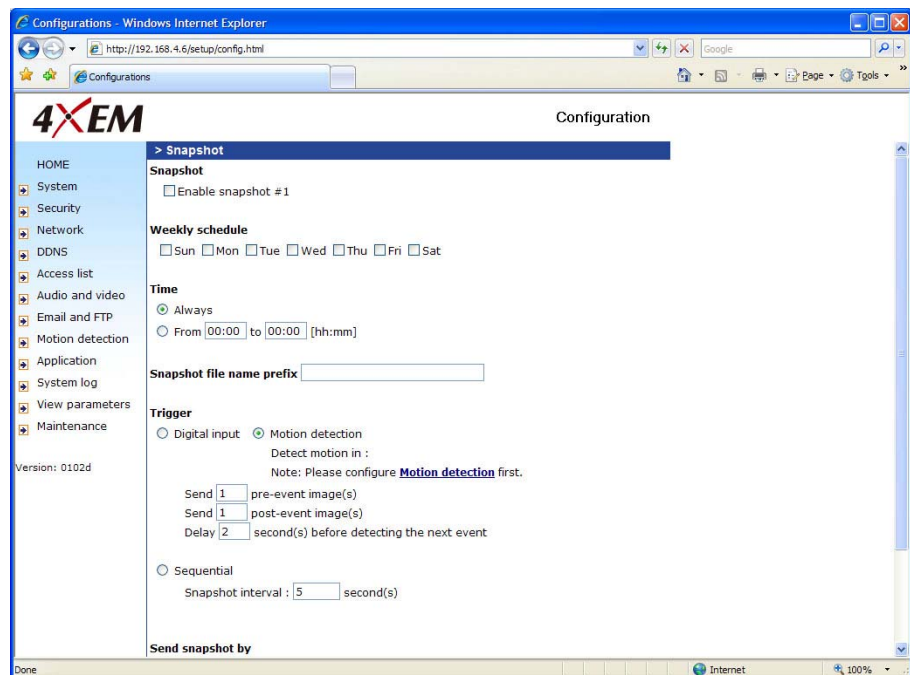
Snapshot

Enable snapshot:

Enable/Disable snapshot application.

Weekly Schedule

Sun - Sat: Select the days of the week to perform the application.





IP Surveillance Solutions

Time

Select **Always** or input the time interval.

Snapshot file name prefix

The prefix name will be added on the file name of the snapshot images.

Trigger

Event trigger type has digital input, motion detection and is sequential.

Digital input: Network Camera will send snapshots when the digital input is triggered.

***Note: Please configure Motion Detection first:** There are three windows for motion detection and each needs to be defined. Select the windows which need to be monitored. If motion detection has not been set up, **undefined** will be shown instead of the window title. If this happens, the window can be defined by clicking on [Motion detection](#) and a note will show to direct the user to the configuration page for motion detection setup.

[Motion Detection](#)

See Motion Detection (page 25) for set-up instructions.

Send pre-event image(s): The number of pre-snapshots that will be captured and sent when a condition is triggered.

Send post-event image(s): The number of post-snapshots that will be captured and sent when a condition is triggered.

Delay second(s) before detecting next motion: Set the time delay before restarting to check on the triggering condition when the current condition is triggered.

Sequential: Snapshot interval: second(s): The Network Camera will send snapshots at the specified intervals to the external server using the method selected below. Remember: This operation is still subject to the conditions set in the weekly schedule.

Send Snapshot By

Email: This selects the uploading method following the intervals set above. The snapshot named "prefix-yyyymmdd-hhmmss.jpg" will be attached in the email.

FTP: The snapshots will be uploaded to the external FTP server with the file name defined in the next option. This can also be used to refresh the captured images stored in the external web server to build creative homepages.

FTP put snapshots with date and time suffix: This option sets up the snapshot capture

date and time, which can be used to easily differentiate the snapshot file names in the sequential operation. For instance, "prefix-20030102-030405.jpg" means the JPEG image was captured in the year 2003, January the 2nd, at 3 o'clock, 4 minute, and 5 second. If this suffix is omitted, the file named "video.jpg" on the external FTP server will be refreshed at the specified interval.

Video Clip

Video Clip

Enable videoclip:

Enable/Disable video clip application.

Weekly Schedule

Sun – Sat: Select the days of the week to perform the application.

Time

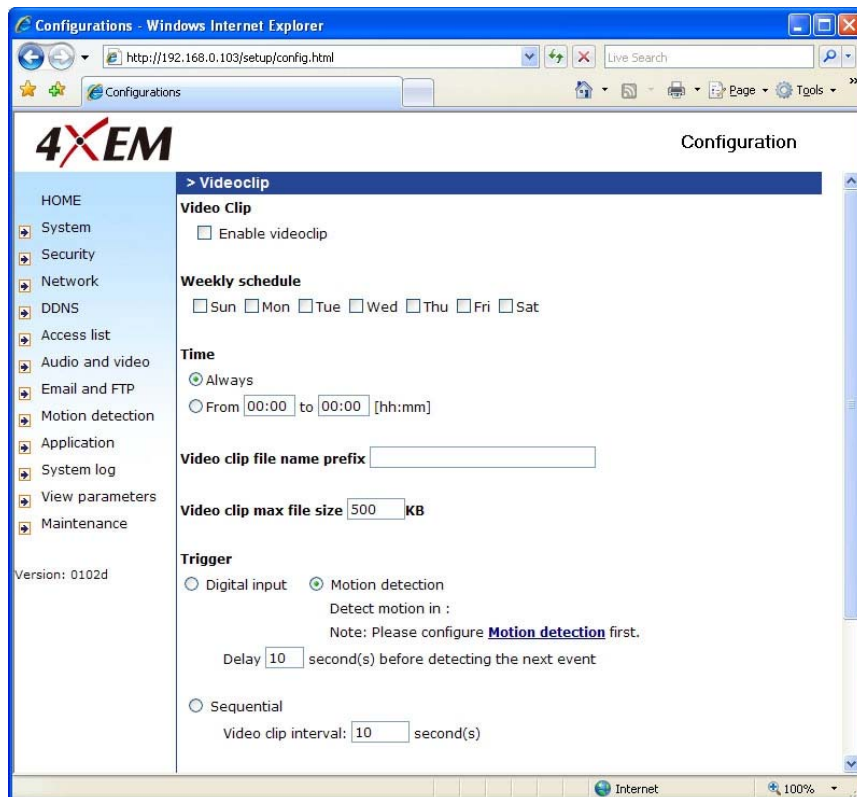
Select **Always** or input the time interval.

Video clip file name prefix

The prefix name will be added on the file name of the video clip files.

Video clip max file size

Define the maximum size of one video clip file.





IP Surveillance Solutions

Trigger

Digital input: The Network Camera will send video clip file when the digital input is triggered.

***Note: Please configure Motion Detection first:** There are three windows for motion detection and each needs to be defined. Select the windows which need to be monitored. If motion detection has not been set up, **undefined** will be shown instead of the window title. If this happens, the window can be defined by clicking on [Motion detection](#) and a note will show to direct the user to the configuration page for motion detection setup.

Delay second(s) before detecting next event: Set the time delay before restarting to check on the triggering condition when the current condition is triggered.

Sequential: Video clip interval: second(s): The Network Camera will send the video clip file at the specified intervals to the external server using the method selected below. Remember: This operation is still subject to the conditions set in the weekly schedule.

Send Videoclip By

Email: This selects the uploading method following the intervals set above. The snapshot named "prefix-yyyymmdd-hhmmss.jpg" will be attached in the email.

FTP: The snapshots will be uploaded to the external FTP server with the file name defined in the next option. This can also be used to refresh the captured images stored in the external web server to build creative homepages.

FTP put snapshots with date and time suffix: This option sets up the snapshot capture date and time, which can be used to easily differentiate the snapshot file names in the sequential operation. For instance, "prefix-20030102-030405.jpg" means the JPEG image was captured in the year 2003, January the 2nd, at 3 o'clock, 4 minute, and 5 second. If this suffix is omitted, the file named "video.jpg" on the external FTP server will be refreshed at the specified interval.

Digital Output

Digital Output

Enable digital output:

Enable/Disable digital output application.

Weekly Schedule

Sun – Sat: Select the days of the week to perform the application.

Time

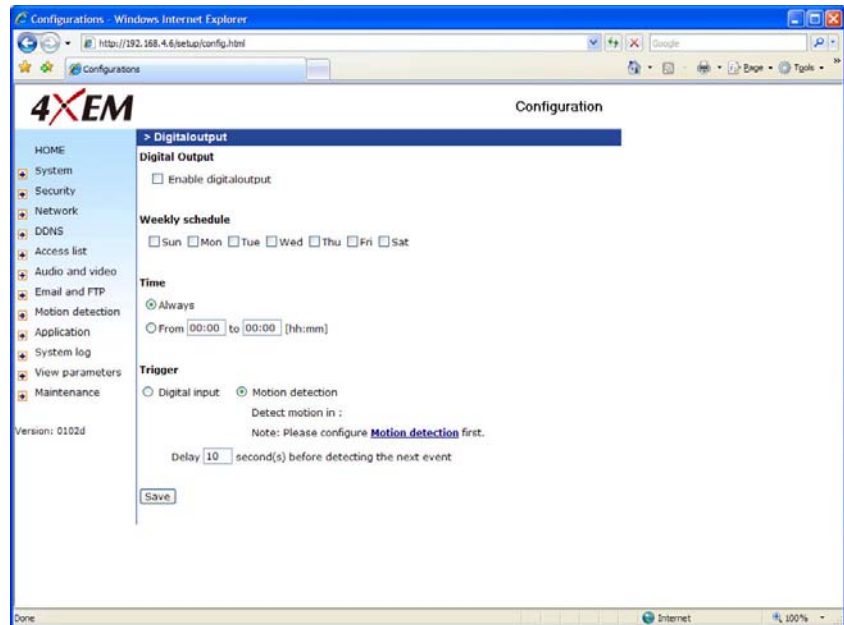
Select **Always** or input the time interval.

Trigger

Digital input: The Network Camera will send video clip file when the digital input is triggered.

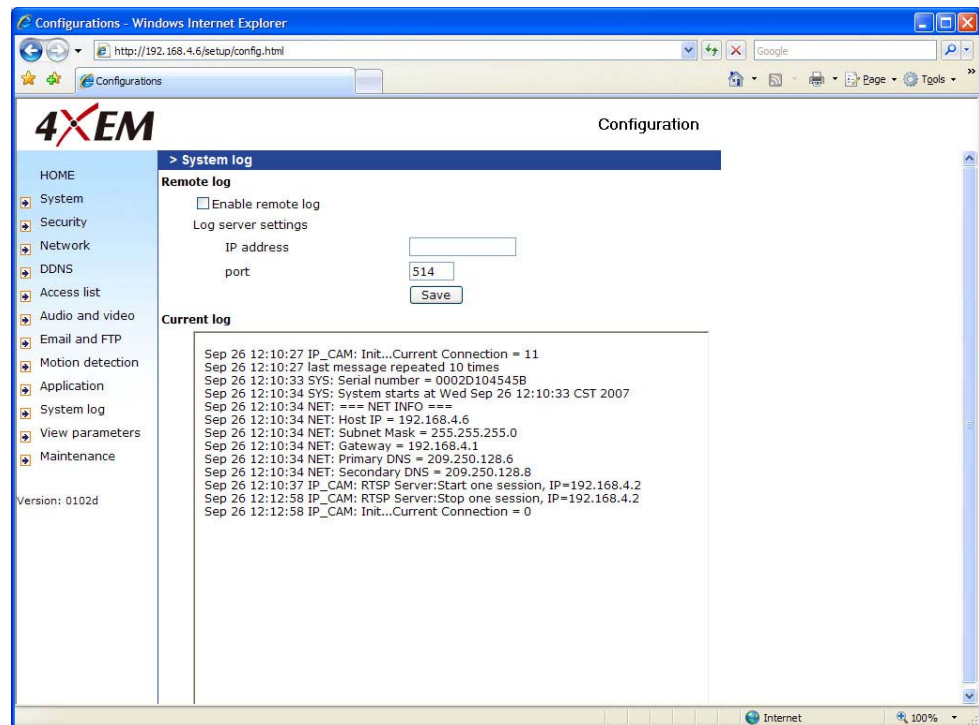
***Note: Please configure Motion Detection first:** There are three windows for motion detection and each needs to be defined. Select the windows which need to be monitored. If motion detection has not been set up, **undefined** will be shown instead of the window title. If this happens, the window can be defined by clicking on [Motion detection](#) and a note will show to direct the user to the configuration page for motion detection setup.

Delay second(s) before detecting next event: Set the time delay before restarting to check on the triggering condition when the current condition is triggered.



System Log

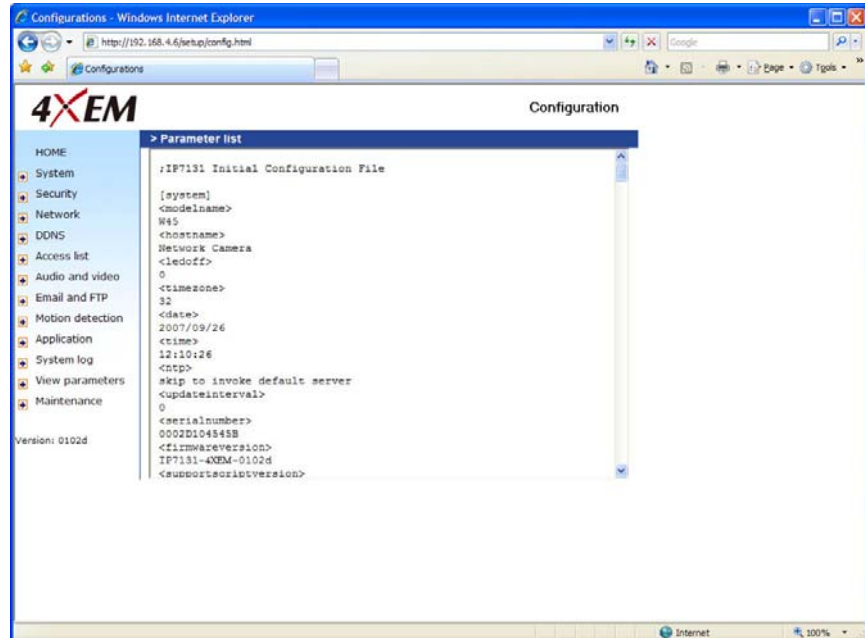
The Network Camera contains a system log where all system related messages for the camera can be viewed. This system log contains important information about the configuration and connection of the camera after bootup. Remote logging is also possible on a Linux server with syslogd service running. Simply enter the IP Address and Port Number of the server to configure the remote logging option. Please note: your remote server must be RFC 3164 compliant.



Check **Enable remote log** and input the **IP address** and **port** number of the log server to enable the remote log facility. **Current log** displays the current system log file. The content of the log provides useful information about configuration and connection after system boot-up.

Viewing System Parameters

Click on this link on the configuration page to view the entire system's parameter set. The content is the same as those in CONFIG.INI.



Maintenance

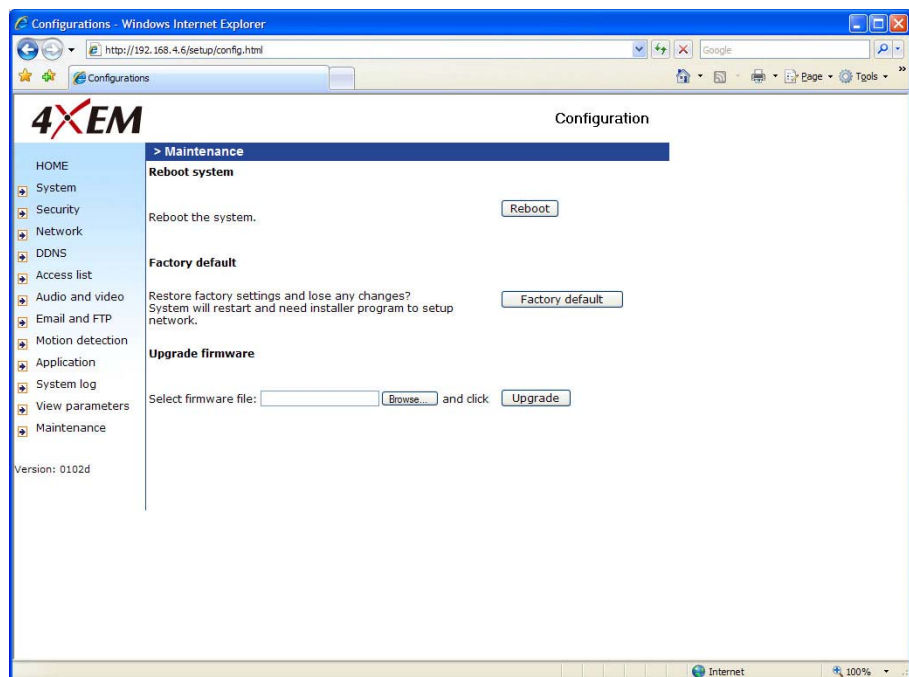
Three actions can be selected.

Reboot: Click the reboot button to restart the system.

Factory default: Click on the Factory Default button on the configuration page to restore the factory default settings. Any changes made will be lost and the system will be reset to the initial factory settings. The system will

restart and require the installer program to set up the network again.

Upgrade firmware: Select the firmware file and click upgrade button.



Appendix

A. Troubleshooting

Status LED

The following table lists the LED patterns which indicate camera status.

Status LED Color	Description
Blinking Red	Power is being supplied to the camera.
Steady Green	The camera is booting up.
Blinking Orange & Green	The camera is trying to obtain an IP address.
Steady Orange	An IP address is successfully assigned to the camera.
Blinking Orange & Red	The camera is working.
Fast Blinking Orange & Red	During firmware upgrading.

Reset and Restore

There is a button in the back of the Network Camera. It is used to reset the system or restore the factory default settings. Sometimes resetting the system sets the system back to normal state. If the system problems remain after reset, restore the factory settings and install again.

RESET: Click on the button.

RESTORE:

1. Press on the button continuously.
2. Wait for self-diagnostic to run twice.
3. Free the button as soon as the second self-diagnostic starts.



Restoring the factory defaults will erase any previous settings. Reset or restore the system after power on.

B. URL Commands of the Network Camera

For some customers who already have their own web site or web control application, the Network Camera can be easily integrated through convenient URLs. This section lists the commands in URL format corresponding to the basic functions of the Network Camera.

Get server parameter values

Note: This request requires administrator access

Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/admin/getparam.cgi?[<parameter>]  
[&<parameter>...]
```

Where the *<parameter>* should be *<group>[_<name>]* or *<group>[.<name>]* If you do not specify the any parameters, all the parameters on the server will be returned. If you specify only *<group>*, the parameters of related group will be returned.

When query parameter values, the current parameter values are returned.

Successful control requests returns parameter pairs as follows.

Return:

```
HTTP/1.0 200 OK\r\n  
Content-Type: text/html\r\n  
Context-Length: <length>\r\n  
\r\n  
<parameter pair>
```

where *<parameter pair>* is

<parameter>=<value>\r\n

[<parameter pair>]

<length> is the actual length of content.



Example: request IP address and its response

Request:

http://192.168.0.123/cgi-bin/admin/getparam.cgi?network_ipaddress

Response:

HTTP/1.0 200 OK\r\n

Content-Type: text/html\r\n

Context-Length: 33\r\n

\r\n

network.ipaddress=192.168.0.123\r\n

Set server parameter values

Note: This request require administrator access

Method: GET/POST

Syntax:

http://<servername>/cgi-bin/admin/setparam.cgi?

[nosync= <value>]& <parameter>=<value>

[&<parameter>=<value>...][&return=<return page>]

parameter	value	description
<group>_<name>	value to assigned	Assign <value> to the parameter <group>_<name>..
return	<return page>	Redirect to the page <return page> after the parameter is assigned. The <return page> can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page. (note: The return page can be a general HTML file(.htm, .html) or a 4XEM server script executable (.vspx) file. It can not be a CGI command. It can not have any extra parameters. This parameter must be put at end of parameter list)



IP Surveillance Solutions

Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: text/html\r\n
Context-Length: <length>\r\n
\r\n
<parameter pair>
```

where <parameter pair> is
<parameter>=<value>\r\n

[<parameter pair>]

Only the parameters that you set and are readable will be returned.

Example: Set the IP address of server to 192.168.0.123

Request:

http://myserver/cgi-bin/admin/setparam.cgi?Network_IPAddress=192.168.0.123

Response:

```
HTTP/1.0 200 OK\r\n
Content-Type: text/html\r\n
Context-Length: 33\r\n
\r\n
network.ipaddress=192.168.0.123\r\n
```

Available parameters on the server

NOTE: The bold characters in table are the default value of each parameter.

Group: **System**

NAME	VALUE	DESCRIPTION
hostname (r/w)	<text string shorter than 40 characters>	host name of server << Wireless > Network Camera >
ledoff (r/w)	0	Do not turn off the led indicator
	1	Turn off the led indicator



IP Surveillance Solutions

date (r/w)	<yyyy/mm/dd>	year, month and date separated by slash.
	<keep>	Keep date unchanged
	<auto>	Using NTP to sync date/time automatically
time (r/w)	<hh:mm:ss>	hour, minute and second separated by colon.
	<keep>	keep date unchanged
	<auto>	Using NTP to sync date/time automatically
ntp (r/w)	<domain name or IP address>	NTP server <skip to invoke default server>
timezone (r/w)	-12 ~ 12	time zone, 8 means GMT +8:00 <8>
updateinterval (r/w)	0 ~ 2592000	0 to Disable automatic time adjustment, otherwise, it means the seconds between NTP automatic update interval. <0>
serialnumber (r)	<mac address>	12 characters mac address without hyphen connected
firmwareversion (r)	<text string shorter than 39 characters>	The version of firmware, including model, company, and version number
restore (w)	0	Restore the system parameters to default value.
	Positive integer	Restore the system parameters to default value and restart the server after <value> seconds.
reset (w)	0 ~ 65535	Restart the server after <value> seconds.
	-1	Not restart the server.
viewmode (r/w)	0	Using the profile of viewing by computer
	1	Using the profile of viewing by mobile phone

Group: Security

NAME	VALUE	DESCRIPTION
username_<1~20> (r/w)	<text string shorter than 16 characters>	change user name. <blank>



IP Surveillance Solutions

userpass_<0~20> (r/w)	<text string shorter than 14 characters>	change user's password. The UserPass_0 is root's password. <blank>
userattr_<1~20> (r)	[conf]	show user's privilege. The privilege can be <blank> - only permit to view live media conf – Permit to change server's configuration <blank>
usercount (r)	1 ~ 21	The current account number on the server including root.<1>

Group: Network

NAME	VALUE	DESCRIPTION
type (r/w)	0	LAN
	1	PPPoE
pppoeuser (r/w)	<text string shorter than 80 characters>	PPPoE account user name <blank>
pppoepass (r/w)	<text string shorter than 15 characters>	PPPoE account password <blank>
resetip (r/w)(restart)	1	enable to get ipaddress, subnet, router, dns1, dns2 from DHCP server at next reboot
	0	Using preset ipaddress, subnet, router, dns1, dns2
ipaddress (r/w) (restart)	<IP address>	IP address of server <192.168.0.99>
subnet (r/w) (restart)	<IP address>	subnet mask <255.255.255.0>
router (r/w) (restart)	<IP address>	default gateway <blank>
dns1 (r/w) (restart)	<IP address>	primary DNS server <blank>
dns2 (r/w) (restart)	<IP address>	secondary DNS server <blank>
smtp1 (r/w)	<domain name or IP address, string shorter than 40 characters>	primary SMTP server <blank>



IP Surveillance Solutions

mailto1 (r/w)	<string shorter than 80 characters>	mail recipient address <blank>
mailuser1 (r/w)	<text string shorter than 63 characters>	User name of primary smtp server <blank>
mailpass1 (r/w)	<text string shorter than 15 characters>	Password of primary smtp server <blank>
smtp2 (r/w)	<domain name or IP address, string shorter than 40 characters>	secondary SMTP server <blank>
mailto2 (r/w)	<text string shorter than 80 characters>	mail recipient address <blank>
mailuser2 (r/w)	<text string shorter than 63 characters>	User name of secondary smtp server <blank>
mailpass2 (r/w)	<text string shorter than 15 characters>	Password of secondary smtp server <blank>
returnemail (r/w)	<text string shorter than 80 characters>	return email address <blank>
localftpport (r/w)	<positive number less than 65535>	FTP port <21>
ftp1 (r/w)	<domain name or IP address, string shorter than 40 characters >	primary FTP server <blank>
ftpport1 (r/w)	<positive number less than 65535>	primary FTP port <21>
ftpuser1 (r/w)	<text string shorter than 63 characters>	user name for primary FTP server <blank>
ftppass1 (r/w)	<text string shorter than 15 characters>	password for primary FTP server <blank>
ftpfolder1 (r/w)	<text string shorter than 40 characters>	upload folder in primary FTP server <blank>
ftppasvmode1 (r/w)	1	Enable passive mode of primary FTP server
	0	Disable passive mode of primary FTP server
ftp2 (r/w)	<domain name or IP address, string shorter than 40 characters >	secondary FTP server



IP Surveillance Solutions

ftpport2 (r/w)	<positive number less than 65535>	secondary FTP port <21>
ftpuser2 (r/w)	<text string shorter than 63 characters>	user name for secondary FTP server <blank>
ftppass2 (r/w)	<text string shorter than 15 characters>	password for secondary FTP server <blank>
ftpfolder2 (r/w)	<text string shorter than 40 characters>	upload folder in secondary FTP server <blank>
ftppasvmode2 (r/w)	1	Enable passive mode of primary FTP server
	0	Disable passive mode of primary FTP server
httpport (r/w) (restart)	<positive number less than 65535>	HTTP port <80>
rtspport (r/w) (restart)	<positive number less than 65535>	RTSP port <554>
videoport (r)	<positive number less than 65535>	video Channel port for RTP <5558>
audioport (r)	<positive number less than 65535>	audio Channel port for RTP <5556>
accessname (r/w)	<text string shorter than 20 characters>	RTSP access name <live.sdp>

Group: IPFilter

NAME	VALUE	DESCRIPTION
allowstart_<0~9> (r/w)	1.0.0.0 255.255.255.255	~ Allowed starting RTSP connection IP address <1.0.0.0>
allowend_<0~9> (r/w)	1.0.0.0 255.255.255.255	~ Allowed ending RTSP connection IP address <255.255.255.255>
denystart_<0~9> (r/w)	1.0.0.0 255.255.255.255	~ Denied starting RTSP connection IP address <blank>
denyend_<0~9> (r/w)	1.0.0.0 255.255.255.255	~ Denied ending RTSP connection IP address <blank>

Group: Video

NAME	VALUE	DESCRIPTION
text	<text string shorter	enclosed caption



IP Surveillance Solutions

(r/w)	than 14 characters>	< blank >
codectype	0	MPEG4
(r/w)	1	MJPEG
keyinterval	1, 3, 5, 10, 30, 60, 90,	Key frame interval
(r/w)	120	< 60 >
size	1	half
(r)	2	half x 2
	3	normal
	4	normal x 2
	5	double
	256	This field is obsolete (use resolution)
resolution	176x144 (for mobile)	Video resolution 176 x 144
(r/w)	160x120	Video resolution 160 x 120
	320x240	Video resolution 320 x 240
	640x480 (for computer)	Video resolution 640 x 480
color	0	monochrome
(r/w)	1	color
quality	0	fix bit rate
(r/w)	1	fix quantization
quant	1	lowest quality of video
(r/w)	2	lower quality of video
	3	normal quality of video
	4	higher quality of video
	5	highest quality of video
bitrate	20000	set bit rate to 20K bps
(r/w)	30000	set bit rate to 30K bps
	40000	set bit rate to 40K bps
	50000	set bit rate to 50K bps
	64000	set bit rate to 64K bps
	128000	set bit rate to 128K bps
	256000	set bit rate to 256K bps
	512000	set bit rate to 512K bps
	768000	set bit rate to 768K bps



IP Surveillance Solutions

	1000000	set bit rate to 1000K bps
	1500000	set bit rate to 1500K bps
	2000000	set bit rate to 2000K bps
	3000000	set bit rate to 3000K bps
	4000000	set bit rate to 4000K bps
maxframe (r/w)	1	set maximum frame rate to 1 fps
	2	set maximum frame rate to 2 fps
	3	set maximum frame rate to 3 fps
	5	set maximum frame rate to 5 fps
	10	set maximum frame rate to 10 fps
	15	set maximum frame rate to 15 fps
	20	set maximum frame rate to 20 fps
	25	set maximum frame rate to 25 fps
	30 (for 60Hz only)	set maximum frame rate to 30 fps
mode (r/w) (in CMOS version only)	50	synchronize with 50Hz utility
	60	synchronize with 60Hz utility
whitebalance (r/w) (in CMOS version only)	0	auto white balance
	1	fixed indoor(3200K)
	2	fixed fluorescent (5500K)
	3	fixed outdoor(> 5500K)
flip (r/w)	1	flip image
	0	normal image
mirror (r/w)	1	mirror image
	0	normal image
imprinntimestam p (r/w)	1	Overlay time stamp on video
	0	Do not overlay time stamp on video

Group: **Audio**

NAME	VALUE	DESCRIPTION
type (r/w)	AAC4 (for computer)	set codec to AAC
	GAMR (for mobile)	set codec to GSM-AMR
aacbitrate	16000	set AAC bitrate to 16K bps

(r/w)	32000	set AAC bitrate to 32K bps
	48000	set AAC bitrate to 48K bps
	64000	set AAC bitrate to 64K bps
	96000	set AAC bitrate to 96K bps
	128000	set AAC bitrate to 128K bps
amrbitrate (r/w)	4750	set AMR bitrate to 4.75K bps
	5150	set AMR bitrate to 5.15K bps
	5900	set AMR bitrate to 5.9K bps
	6700	set AMR bitrate to 6.7K bps
	7400	set AMR bitrate to 7.4K bps
	7950	set AMR bitrate to 7.95K bps
	10200	set AMR bitrate to 10.2K bps
	12200	set AMR bitrate to 12.2K bps

Group: Image

NAME	VALUE	DESCRIPTION
brightness (r/w)	<-5 ~ 5>	Adjust brightness of image according to mode settings. <0>
saturation (r/w)	<-5 ~ 5>	Adjust saturation of image according to mode settings. <0>
contrast (r/w)	<-5 ~ 5>	Adjust contrast of image according to mode settings. <0>
hue (r/w)	<-5 ~ 5>	Adjust hue of image according to mode settings. <0>

Group: Motion

NAME	VALUE	DESCRIPTION
enabled (r/w)	0	disable motion detection
	1	enable motion detection
winenabled_<0~2> (r/w)	0	disable motion window #1
	1	enable motion window #1
winname_<0~2> (r/w)	<text string shorter than 14 characters >	name of motion window #1 <blank>
winleft_<0~2> (r/w)	0 ~ 320	Left coordinate of window position. <0>



IP Surveillance Solutions

wintop_<0~2> (r/w)	0 ~ 240	Top coordinate of window position. <0>
winwidth_<0~2> (r/w)	0 ~ 320	Width of motion detection window. <0>
winheight_<0~2> (r/w)	0 ~ 240	Height of motion detection window. <0>
winobjsize_<0~2> (r/w)	0 ~ 100	Percent of motion detection window <0>
winsensitivity_<0~2> > (r/w)	0 ~ 100	Sensitivity of motion detection window <0>
update (w)	1	Update the above motion detection settings to take effect

Group: DDNS

NAME	VALUE	DESCRIPTION
enable (r/w)	0, 1	Enable or disable the dynamic dns. <0>
provider (r/w)	1 ~ 6	dyndns.org (dynamic) dyndns.org (custom) tzo.com dhs.org safe100.net dyn-interfree.it <1>
hostname (r/w)	Text string shorter than 127 characters.	Your dynamic hostname. <blank>
usernameemail (r/w)	Text string shorter than 63 characters.	Your user or email to login ddns service provider <blank>
passwordkey (r/w)	Text string shorter than 20 characters.	Your password or key to login ddns service provider <blank>
update (w)	0, 1	Update the above ddns settings to take effect

Group: **UPNP**

NAME	VALUE	DESCRIPTION
enable (r/w)	0, 1	Enable or disable the UPNP presentation service. <1>

Group: **UPNPfor**

NAME	VALUE	DESCRIPTION
enable (r/w)	0, 1	Enable or disable the UPNP port forwarding service. <0>

Group: **App**

NAME	VALUE	DESCRIPTION
scriptname (r)	<text string shorter than 255 characters>	File name of script <script.vssx>
enablescript (r/w)	0	Disable script
	1	Enable script

Group: **Syslog**

NAME	VALUE	DESCRIPTION
enableremotelog (r/w)	0	disable remote log
	1	enable remote log
serverip (r/w)	<IP address>	Log server IP address
serverport (r/w)	<514>	Server port used for log

Application page CGI command

Note: This request requires administrator privilege.

Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/admin/gen-eventd-conf.cgi?[ snapshot_enable=<value>]
[&weekday=<value>][&time_method=<value>][&begin_time=<value>]
[&end_time=<value>]
[&ss_prefix=<value>][&trigger_type=<value>]
[&md_prenum=<value>][&md_postnum=<value>][&md_delay=<value>]
[&sq_interval=<value>]
[&send_method=<value>][&ftp_suffix=<value>]
```

Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: <length>\r\n
\r\n
<depends on method value>
If(method == get || method == set)
{
    tue=<value>\r\n
    wed=<value>\r\n
    ...
}
Else if(method == normal)
{
    Application page contents
}
```

parameter	Value	description
snapshot_enable	0	Enable snapshot application
	1	Disable snapshot application
weekday	0,1,2,3,4,5,6	The array indicate weekly schedule
time_method	<i>always</i>	24 hours full day
	<i>interval</i>	Select begin time and end time
begin_time	<i>hh:mm</i>	Begin time of weekly schedule



IP Surveillance Solutions

end_time	<i>hh:mm</i>	End time of weekly schedule
ss_prefix	<i><text string shorter than 60 characters></i>	Snapshot file name prefix for both event and sequential operation
trigger_type	<i>motion</i>	Set trigger by motion detect
	<i>sequential</i>	Snapshot sequentially
md_win	<i>0,1,2</i>	The array indicate which motion windows are used
md_prenum	<i>1~5</i>	The numbers of snapshot before event
md_postnum	<i>1~5</i>	The numbers of snapshot after event
md_delay	<i>1~999</i>	The delay seconds for detecting next motion event
sq_interval	<i>1~999</i>	The interval seconds of sequential snapshot
send_method	<i>mail</i>	Send snapshot by mail
	<i>ftp</i>	Send snapshot by ftp
ftp_suffix	<i>0/1</i>	Enable/Disable file name prefix

Capture single snapshot

Note: This request require normal user privilege

Method: GET/POST

Syntax:

<http://<servername>/cgi-bin/video.jpg>

Server will return the most up-to-date snapshot in JPEG format. The size and quality of image will be set according to the video settings on the server.

Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: image/jpeg\r\n
[Content-Length: <image size>\r\n]

<binary JPEG image data>
```

Account management

Note: This request requires administrator privilege

Method: GET/POST

Syntax:

[http://<servername>/cgi-bin/admin/editaccount.cgi?](http://<servername>/cgi-bin/admin/editaccount.cgi?method=<value>&username=<name>[&userpass=<value>][&privilege=<value>][&privilege=<value>][...][&return=<return page>])
method=<value>&username=<name>[&userpass=<value>][&privilege=<value>]
[&privilege=<value>][...][&return=<return page>]

parameter	value	Description
method	add	Add an account to server. When using this method, "username" field is necessary. It will use default value of other fields if not specified.
	delete	Remove an account from server. When using this method, "username" field is necessary, and others are ignored.
	edit	Modify the account password and privilege. When using this method, "username" field is necessary, and other fields are optional. If not specified, it will keep original settings.
username	<name>	The name of user to add, delete or edit
userpass	<value>	The password of new user to add or that of old user to modify. The default value is an empty string.
privilege	<value>	The privilege of user to add or to modify. The privilege can be the addition of the following values. Ex: A user with configure access can be assigned privilege as privilege=conf .
	conf	configuration privilege
return	<return page>	Redirect to the page <return page> after the parameter is assigned. The <return page> can be a full URL path or relative path according the the current path. If you omit this parameter, it will redirect to an empty page.



IP Surveillance Solutions

System Logs

Note: This request require administrator privilege

Method: GET/POST

Syntax:

<http://<servername>/cgi-bin/admin/syslog.cgi>

Server will return the up-to-date system log.

Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: <syslog length>\r\n
\r\n
<system log information>\r\n
```

Configuration file

Note: This request requires administrator privilege

Method: GET/POST

Syntax:

<http://<servername>/cgi-bin/admin/configfile.cgi>

Server will return the up-to-date configuration file.

Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: <configuration file length>\r\n
\r\n
<configuration data>\r\n
```



IP Surveillance Solutions

Upgrade Firmware

Note: This request requires administrator privilege

Method: POST

Syntax:

<http://<servername>/cgi-bin/admin/upgrade.cgi>

Post data:

fimage=<file name> [&return=<return page>] \r\n
\r\n
<multipart encoded form data>

Server will accept the upload file named <file name> to be upgraded the firmware and return with <return page> if indicated.

C. Technical Specifications

System

CPU: VVTK-1000
RAM: 32MB SDRAM
ROM: 4MB FLASH ROM
Image Sensor: VGA CMOS
Embedded OS: Linux2.4

Networking

Protocols

TCP/IP, HTTP, SMTP, FTP, DDNS, UPnP, Telnet, NTP, DNS, DHCP and RTSP

Physical

10/100 baseT Fast Ethernet auto negotiation

Video

Algorithm supported

MPEG4(simple profile) for streaming video
JPEG for still image

Features

Adjustable image size, quality and bit rate
Time stamp and text overlay
3 motion detection windows

Resolution

Up to 30/25 frames at 160x120
Up to 30/25 frames at 320x240
Up to 30/25 frames at 640x480

Camera Specification

1/4 inch color CMOS sensor
Resolution: 640x480
1.5Lux/F2.0
AGC, AWB, AES
Electronic shutter: 1/60 ~ 1/15000 second

Lens

Fixed focal with fine tuning, 4.0mm, F2.0

Stream

MPEG-4 streaming over UDP, TCP, or HTTP
MPEG-4 multicast streaming

Event Management

Multiple-window video motion detection
1 digital input and 1 digital output
Event notification using HTTP, SMTP, or FTP

Audio

Supports GSM-AMR

Supports AAC compression

Supports audio mute

Bit rate:

GSM-AMR: 4.75k~12.2k

ACC: 15k~128k

Security

Multi-level user access

IP address filtering

LED indicator

Bi-color LED system status indicator

Dimension

126.4mm (L) x 96.2mm (W) x 47.4mm (H)

Weight

NET. 276g

Power

12V DC
Power over Ethernet: 802.3af compliant
Power Consumption: 4.4W

Operating Environment

Temperature: 0-40°C/32-104°F
Humidity: 20%~80% RH

EMI & Safety

CE, FCC, PSE

Application

Installation wizard
16-ch recording software
SDK available for application development and system integration

Viewing system requirement

OS: Microsoft Windows 2000/XP
Browser: Internet Explorer 5.x or above
Cellphone: 3GPP player
Real Player 10.5
Quick Time 6.5
Packet Video Player 3.0

Technology License Notice

AMR Technology

This product includes AMR narrowband speech coding technology licensed by VoiceAge. Please refer to <http://www.voiceage.com/> for more details.

MPEG-4 AAC Technology

This product includes MPEG-4 AAC audio coding technology licensed by Via Licensing. Please refer to <http://www.vialicensing.com/> for more details.

MPEG-4 Visual Technology

This product includes one MPEG-4 encoder and one MPEG-4 decoder license. Installation of more than one decoder is prohibited. Please contact your reseller to purchase additional decoder licenses.

THIS PRODUCT IS LICENSED UNDER THE MPEG-4 VISUAL PATENT PORTFOLIO LICENSE FOR THE PERSONAL AND NON-COMMERCIAL USE OF A CONSUMER FOR (i) ENCODING VIDEO IN COMPLIANCE WITH THE MPEG-4 VISUAL STANDARD ("MPEG-4 VIDEO") AND/OR (ii) DECODING MPEG-4 VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL AND NONCOMMERCIAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED BY MPEG LA TO PROVIDE MPEG-4 VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION INCLUDING THAT RELATING TO PROMOTIONAL, INTERNAL AND COMMERCIAL USES AND LICENSING MAY BE OBTAINED FROM MPEG LA, LLC. SEE [HTTP://WWW.MPEGLA.COM](http://www.mpegla.com).

Electromagnetic Compatibility (EMC)


This device complies with FCC Rules Part 15. Operation is subject to the following two conditions.

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired operation.

USA - This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a partial installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Shielded interface cables must be used in order to comply with emission limits.

Europe  - This digital equipment fulfills the requirement for radiated emission according to limit B of EN55022/1998, and the requirement for immunity according to EN50082-1/1992.

Liability

4XEM Corporation cannot be held responsible for any technical or typographical errors and reserves the right to make changes to the product and manuals without prior notice. 4XEM Corporation makes no warranty of any kind with regard to the material contained within this document, including, but not limited to, the implied warranties of merchantability and fitness for any particular purpose.